CHAPTER 10

ブロッキングとレート制限のための ARC の設定

この章では、Attack Response Controller（ARC）がセンサー上でブロッキングとレート制限を実行するように設定する方法について説明します。

（注） ARC は、以前は Network Access Controller と呼ばれていました。この名前は IPS 5.1 で変更されましたが、CLI には現在も `nac` や `network-access` などの用語が存在します。

この章は、次の項で構成されています。

ブロッキングについて

センサー上のブロッキング アプリケーションである ARC は、ルータ、スイッチ、PIX ファイアウォール、FWSM、および ASA でブロックを開始および停止します。ARC は、管理しているデバイス上で IP アドレスをブロックします。ARC は、他のマスター ブロッキング センサーも含めて、管理しているすべてのデバイスに同じブロックを送信します。ARC はブロックの時間を監視し、その時間が満了するとブロックを削除します。

注意　FWSM がマルチモードで設定されている場合、管理コンテキストではブロッキングはサポートされません。ブロッキングは、シングルモードおよびマルチモードのカスタマー コンテキストでのみサポートされます。

（注）　ARC は、新しいブロックに対するアクション応答を 4 ～ 7 秒以内に完了するように設計されています。ほとんどの場合、より短い時間でアクション応答を完了します。このパフォーマンス上の目標を実現するため、センサーでは、過度なレートでのブロックの実行やデバイスとインターフェイスに対する過剰なブロックの管理を設定しないでください。ブロックの最大数は 250 未満、ブロックする項目の最大数は 10 未満にすることをお勧めします。ブロックする項目の最大数を計算する場合は、ファイアウォール、ASA、または FWSM を、ブロックするコンテキストごとに 1 つのブロックする項目として数えます。ルータは、ブロックするインターフェイス / 方向ごとに 1 つのブロックする項目として数えます。Catalyst ソフトウェアを実行するスイッチは、ブロックする VLAN ごとに 1 つのブロックする項目として数えます。推奨される制限を越えると、ARC がブロックをちょうどよいタイミングで適用しなかったり、ブロックをまったく適用しなかったりする可能性があります。

マルチモードで設定された ASA、PIX Firewall 7.0、FWSM 2.1 以降などのファイアウォールの場合、IPS 5.1 はブロック要求に VLAN 情報を挿入しません。このため、ブロックされている IP アドレスが正しいかどうかをファイアウォールごとに確認する必要があります。たとえば、センサーが VLAN A 用に設定されたファイアウォールのカスタマー コンテキストでパケットを監視し、VLAN B 用に設定された別のファイアウォールのカスタマー コンテキストでブロッキングを実行しているとします。この場合、VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを指している可能性があります。

ブロックには、次の 3 つのタイプがあります。

- ホスト ブロック：特定 IP アドレスからのすべてのトラフィックのブロック。
- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックのブロック。

  同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックを指定すると、そのブロックは接続ブロックからホスト ブロックに自動的に切り替えられます。

  （注）　ファイアウォールでは、接続ブロックはサポートされません。ファイアウォールでは、接続情報を追加したホスト ブロックのみがサポートされます。

- ネットワーク ブロック：特定ネットワークからのすべてのトラフィックのブロック。

  ホスト ブロックと接続ブロックは、シグニチャがトリガーされたときに手動または自動で開始できます。ネットワーク ブロックは、手動でのみ開始することができます。

注意　ブロッキングと、センサーがパケットをドロップする機能を混同しないでください。センサーは、そのセンサーに対して、Deny Packet Inline、Deny Connection Inline、および Deny Attacker Inline アクションがインライン モードで設定されている場合に、パケットをドロップできます。

自動ブロックの場合は、特定のシグニチャのイベント アクションとして **Request Block Host** または **Request Block Connection** を選択し、そのアクションをすべての設定済みイベント アクション オーバーライドに追加する必要があります。この操作により、SensorApp はそのシグニチャがトリガーされたときに ARC にブロック要求を送信することができます。ARC は、SensorApp からブロック要求を受信すると、ホストまたは接続をブロックするようにデバイス コンフィギュレーションを更新します。Request Block Host または Request Block Connection イベント アクションをシグニチャに追加する手順については、P.7-13 の「シグニチャへのアクションの割り当て」を参照してください。また、特定のリスク評価のアラームに Request Block Host または Request Block Connection イベント アクションを追加するオーバーライドを設定する手順については、P.6-11 の「イベント アクション オーバーライドの設定」を参照してください。

Cisco ルータおよび Catalyst 6500 シリーズ スイッチでは、ARC は ACL または VACL を適用することによってブロックを作成します。ACL と VACL は、インターフェイスの方向または VLAN 上のデータ パケットの追加を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可または拒否の条件が記述されています。PIX Firewall、FWSM、および ASA では、ACL または VACL は使用されません。組み込みの **shun** および **no shun** コマンドが使用されます。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新規 ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。詳細については、P.10-26 の「センサーがデバイスを管理するしくみ」を参照してください。

ARC でデバイスを管理するには、次の情報が必要です。

- ログイン ユーザ ID（デバイスに AAA が設定されている場合）
- ログイン パスワード
- イネーブル パスワード（ユーザがイネーブル特権を持っている場合は不要）
- 管理対象のインターフェイス（ethernet0、vlan100 など）
- 作成される ACL または VACL で、最初に適用する任意の既存 ACL または VACL 情報（Pre-Block ACL または VACL）、または最後に適用する ACL または VACL 情報（Post-Block ACL または VACL）

  この情報は、PIX Firewall、FWSM、および ASA には適用されません。これらはブロックに ACL を使用しないためです。
- デバイスとの通信で Telnet または SSH を使用するかどうか
- ブロックしない IP アドレス（ホストまたはホストの範囲）
- ブロックを続ける期間

ヒント　ARC のステータスを確認するには、`sensor#` で **show statistics network-access** と入力します。これにより、管理しているデバイス、アクティブなブロック（存在する場合）、およびすべてのデバイスのステータスが表示されます。または、IDM で **Monitoring > Statistics** をクリックして ARC のステータスを表示します。

（注）　ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されていますが、IDM と CLI には Network Access Controller を指す **nac** や **network-access** などの表記が存在します。

レート制限について

レート制限により、センサーはネットワーク デバイス上の指定されたトラフィック クラスのレートを制限することができます。レート制限の応答は、Host Flood エンジンと Net Flood エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC は、Cisco IOS バージョン 12.3 以降を実行するネットワーク デバイスでレート制限を設定することができます。ルータでのレート制限の設定については、P.10-26 の「ブロッキング デバイスおよびレート制限デバイスの設定」を参照してください。マスター ブロッキング センサーは、レート制限要求をブロッキング転送センサーに転送することもできます。詳細については、P.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」を参照してください。

アクティブなレート制限のリストは、ARC の統計情報で確認できます。詳細については、P.13-13 の「統計情報の表示」を参照してください。

レート制限を追加するには、レート制限イベントの生成を許可されたシグニチャのいずれかに一致する、プロトコル、宛先 IP アドレス、およびデータ値の組み合せを指定します。また、アクションを Request Rate Limit に設定し、該当のシグニチャの比率を指定する必要があります。表 10-1 に、サポートされているシグニチャとパラメータを示します。

表 10-1　レート制限のシグニチャ

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
2152	ICMP Flood Host	ICMP	○	echo-request
2153	ICMP Smurf Attack	ICMP	○	echo-reply
4002	UDP Flood Host	UDP	○	なし
6901	Net Flood ICMP Reply	ICMP	×	echo-reply
6902	Net Flood ICMP Request	ICMP	×	echo-request
6903	Net Flood ICMP Any	ICMP	×	なし
6910	Net Flood UDP	UDP	×	なし
6920	Net Flood TCP	TCP	×	なし
3050	TCP HalfOpenSyn	TCP	×	halfOpenSyn

ARC を設定する前の作業

ブロッキングやレート制限を実行するように ARC を設定する前に、必ず次の作業を実行してください。

- ネットワーク トポロジを分析して、どのデバイスをどのセンサーでブロックするかや、ブロックしないアドレスを確認します。

注意　2 つのセンサーが同一のデバイスでブロッキングやレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーを、デバイス管理のためのマスター ブロッキング センサーとして設定します。それにより、もう一方のセンサーはマスター ブロッキング センサーに要求を転送できます。手順については、P.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」を参照してください。

（注）　マスター ブロッキング センサーを追加する場合は、センサーごとにブロックするデバイスの数を減らしてください。たとえば、10 のファイアウォールと 10 のルータでブロッキングを行い、ブロックするインターフェイス / 方向がそれぞれ 1 つずつある場合は、そのうちの 10 をセンサーに割り当て、残りの 10 をマスター ブロッキング センサーに割り当てます。

- 各デバイスにログインするために必要なユーザ名、デバイスのパスワード、イネーブル　パスワード、および接続タイプ（Telnet または SSH）の情報を入手します。
- デバイスのインターフェイス名を確認します。
- 必要に応じて、Pre-Block ACL または VACL、および Post-Block ACL または VACL の名前を確認します。
- ブロックするインターフェイスとブロックしないインターフェイス、およびその方向（インまたはアウト）を確認します。誤ってネットワーク全体を遮断しないでください。

サポートされているデバイス

デフォルトでは、ARC は任意の組み合せで 250 までのデバイスをサポートします。ARC によるブロッキングがサポートされるデバイスは、次のとおりです。

（注） ARC は、新しいブロックに対するアクション応答を 4 ～ 7 秒以内に完了するように設計されています。ほとんどの場合、より短い時間でアクション応答を完了します。このパフォーマンス上の目標を実現するため、センサーでは、過度なレートでのブロックの実行やデバイスとインターフェイスに対する過剰なブロックの管理を設定しないでください。ブロックの最大数は 250 未満、ブロックする項目の最大数は 10 未満にすることをお勧めします。ブロックする項目の最大数を計算する場合は、ファイアウォール、ASA、または FWSM を、ブロックするコンテキストごとに 1 つのブロックする項目として数えます。ルータは、ブロックするインターフェイス / 方向ごとに 1 つのブロックする項目として数えます。Catalyst ソフトウェアを実行するスイッチは、ブロックする VLAN ごとに 1 つのブロックする項目として数えます。

注意 推奨される制限を越えると、ARC がブロックをちょうどよいタイミングで適用しなかったり、ブロックをまったく適用しなかったりする可能性があります。

- Cisco IOS 11.2 以降を使用する Cisco シリーズ ルータ（ACL）
  - Cisco 1600 シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ
- IOS 11.2(9)P 以降を使用する RSM 搭載 Catalyst 5000 スイッチ（ACL）
- IOS 12.1(13)E 以降を使用する Catalyst 6500 スイッチおよび 7600 ルータ（ACL）
- Catalyst ソフトウェア バージョン 7.5(1) 以降を使用する Catalyst 6500 スイッチおよび 7600 ルータ（VACL）
  - PFC 組み込みのスーパーバイザ エンジン 1A
  - MSFC1 組み込みのスーパーバイザ エンジン 1A
  - MFSC2 組み込みのスーパーバイザ エンジン 1A
  - MSFC2 組み込みのスーパーバイザ エンジン 2
  - MSFC3 組み込みのスーパーバイザ エンジン 720

（注） スーパーバイザ エンジンでの VACL ブロッキングと MSFC での ACL ブロッキングがサポートされます。

- バージョン 6.0 以降の PIX Firewall（**shun** コマンド）
  - 501
  - 506E
  - 515E
  - 525
  - 535
- バージョン 7.0 以降の ASA（**shun** コマンド）
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 以降（**shun** コマンド）

ACL、VACL、**shun** コマンドのいずれかを使用してブロッキングを設定できます。すべてのファイアウォールおよび ASA モデルは **shun** コマンドをサポートします。

ARC によるレート制限がサポートされるデバイスは、次のとおりです。

- Cisco IOS 12.3 以降を使用する Cisco シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ

ブロッキング プロパティの設定

デフォルトのブロッキング プロパティを変更することができます。デフォルトのプロパティを使用することをお勧めしますが、変更する必要がある場合は、次の手順を実行します。

センサーによる自らのブロックの許可

センサーが自らをブロックするように設定するには、サービス ネットワーク アクセス サブモードで **allow-sensor-block [true | false]** コマンドを使用します。

注意　センサーが自らをブロックすることは許可しないことをお勧めします。これを許可すると、センサーがブロッキング デバイスと通信しなくなる可能性があります。このオプションは、センサーが自分の IP アドレスをブロックする規則を作成した場合に、そのためにセンサーがブロックしているデバイスにアクセスできなくなることはないと保証されている場合にだけ設定します。

センサーが自らをブロックできるようにするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　センサーが自らをブロックするように設定します。

```
sensor(config-net-gen)# allow-sensor-block true
```

デフォルトでは、この値は **false** です。

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: true default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 11.11.11.11
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 12.12.0.0/16
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 6　センサーが自らをブロックしないように設定します。

```
sensor(config-net-gen)# allow-sensor-block false
```

ステップ 7　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 11.11.11.11
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 12.12.0.0/16
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ブロッキングのディセーブル化

センサーでのブロッキングをイネーブルまたはディセーブルにするには、サービス ネットワーク アクセス サブモードで **block-enable [true | false]** コマンドを使用します。

（注）　ブロッキングが動作するためには、デバイスがブロッキングを実行するように設定する必要があります。手順については、P.10-27 の「センサーで Cisco ルータを管理するための設定」、および P.10-30 の「センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定」を参照してください。

センサーでは、デフォルトでブロッキングがイネーブルになっています。ARC が管理しているデバイスに手動で設定をしなければならない場合は、まずブロッキングをディセーブルにする必要があります。管理者と ARC が同じデバイスに同時に変更を加えないようにしてください。デバイスまたは ARC（またはその両方）がクラッシュするおそれがあります。

注意　デバイスのメンテナンスのためにブロッキングをディセーブルにする場合は、メンテナンスの完了後必ずブロッキングをイネーブルにしてください。これを忘れると、本来ブロックされる攻撃に対してネットワークが脆弱になります。

（注）　ブロッキングがディセーブルの間も、ARC はブロックを受信し続け、アクティブなブロックの時間を把握していますが、管理対象デバイスに対する新しいブロックの適用やブロックの削除は行いません。ブロッキングが再びイネーブルになると、デバイスのブロックが更新されます。

ブロッキングまたはレート制限をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　センサーでのブロッキングをディセーブルにします。

```
sensor(config-net-gen)# block-enable false
```

デフォルトでは、この値は **true** です。

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: false default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 11.11.11.11
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 12.12.0.0/16
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 6　センサーでのブロッキングをイネーブルにします。

```
sensor(config-net-gen)# block-enable true
```

ステップ 7　設定がデフォルトに戻ったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 11.11.11.11
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 12.12.0.0/16
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

最大ブロック数の設定

最大ブロック数を設定するには、サービス ネットワーク アクセス サブモードで **block-max-entries** コマンドを使用します。

同時に維持できるブロックの数を設定することができます（1 ～ 65535）。デフォルト値は 250 です。

注意　250 を超える最大ブロック数を設定することはお勧めしません。一部のデバイスでは、ACL または shun のエントリが多くなると問題が発生する場合があります。この数を増やす前に、各デバイスのマニュアルを参照し、制限を確認してください。

（注）　ブロックの数は、最大ブロック数を超えることはできません。最大数になると、既存のブロックがタイムアウトしてなくなるまで、新しいブロックはできません。

ブロックの最大数を変更するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ブロックの最大数を変更します。

```
sensor(config-net-gen)# block-max-entries 100
```

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 12.12.0.0/16
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 6　デフォルト値である 250 ブロックに戻すには、次のコマンドを実行します。

```
sensor(config-net-gen)# default block-max-entries
```

ステップ 7　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 11.11.11.11
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 12.12.0.0/16
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ブロック時間の設定

自動ブロックが継続する時間を変更するには、サービス イベント アクション ルール サブモードで **global-block-timeout** コマンドを使用します。デフォルトは 30 分です。

（注）　デフォルトのブロック時間を変更すると、シグニチャのパラメータを変更することになるので、すべてのシグニチャが影響を受けます。

（注）　手動ブロックの時間は、ブロックの要求時に設定されます。

デフォルトのブロック時間を変更するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-rul)# general
```

ステップ 4　ブロック時間を設定します。

```
sensor(config-rul-gen)# global-block-timeout 60
```

値は、ブロック イベントの分単位の継続期間です（0 ～ 10000000）。

ステップ 5　設定を確認します。

```
sensor(config-rul-gen)# show settings
   general
   -----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 60 default: 30
      max-denied-attackers: 10000 <defaulted>
   -----------------------------------------------
sensor(config-rul-gen)#
```

ステップ 6　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul-gen)# exit
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 7　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

（注）　シグニチャが更新される間、時間遅延が発生します。

ACL ロギングのイネーブル化

ACL ロギングをイネーブルにするには、サービス ネットワーク アクセス サブモードで **enable-acl-logging [true | false]** コマンドを使用します。ACL ロギングをイネーブルにすると、ARC は ACL または VACL のブロック エントリにログ パラメータを追加します。パケットがフィルタリングされると、デバイスは syslog イベントを生成します。ACL ロギングのイネーブル化は、ルータとスイッチだけに適用されます。デフォルトは disable です。

ACL ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ACL ロギングをイネーブルにします。

```
sensor(config-net-gen)# enable-acl-logging true
```

ステップ 5　ACL ロギングがイネーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: true default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 6　ACL ロギングをディセーブルにするには、**false** キーワードを使用します。

```
sensor(config-net-gen)# enable-acl-logging false
```

ステップ 7　ACL ロギングがディセーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

NVRAM への書き込みのイネーブル化

ARC の最初の接続時にルータが NVRAM への書き込みを実行するようにセンサーを設定するには、**enable-nvram-write [true | false]** コマンドを使用します。enable-nvram-write がイネーブルの場合は、ACL が更新されるたびに NVRAM に書き込みが行われます。デフォルトは disable です。

NVRAM 書き込みをイネーブルにすると、ブロッキングに関するすべての変更が NVRAM に書き込まれます。ルータがリブートされても、正しいブロックがアクティブに保たれます。NVRAM 書き込みがディセーブルの場合は、ルータのリブート後、短時間ですがブロッキングの存在しない状態になります。NVRAM 書き込みをイネーブルにしない場合は、NVRAM の寿命が長くなり、新しいブロックの設定にかかる時間が短くなります。

NVRAM への書き込みをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　NVRAM への書き込みをイネーブルにします。

```
sensor(config-net-gen)# enable-nvram-write true
```

ステップ 5　NVRAM への書き込みがイネーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: true default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　NVRAM への書き込みをディセーブルにします。

```
sensor(config-net-gen)# enable-nvram-write false
```

ステップ 7　NVRAM への書き込みがディセーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

すべてのブロック イベントとエラーのロギング

ブロックの開始から終了までのイベントをログに記録するようにセンサーを設定するには、サービス ネットワーク アクセス サブモードで **log-all-block-events-and-errors [true | false]** コマンドを使用します。たとえば、デバイスにブロックを追加したり、デバイスからブロックを削除したりすると、1 つのイベントがログに記録されます。このようなすべてのイベントやエラーをログに記録する必要のない場合もあります。**log-all-block-events-and-errors** をディセーブルにすると、新しいイベントとエラーが抑止されます。デフォルトは enabled です。

ブロック イベントとエラーのロギングをディセーブルにするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ブロック イベントとエラーのロギングをディセーブルにします。

```
sensor(config-net-gen)# log-all-block-events-and-errors false
```

ステップ 5　ロギングがディセーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: false default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
```

ステップ 6　ブロック イベントとエラーのロギングをイネーブルにします。

```
sensor(config-net-gen)# log-all-block-events-and-errors true
```

ステップ 7　ロギングがイネーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ブロッキング インターフェイスの最大数の設定

ブロックを実行するためのインターフェイスの最大数を設定するには、**max-interfaces** コマンドを使用します。たとえば、PIX Firewall は 1 つのインターフェイスとしてカウントされます。1 つのインターフェイスを持つルータは 1 とカウントされますが、2 つのインターフェイスを持つルータは 2 とカウントされます。デフォルトは 250 です。

ブロッキング インターフェイスの最大数を設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　インターフェイスの最大数を設定します。

```
sensor(config-net-gen)# max-interfaces 50
```

ステップ 5　インターフェイスの最大数を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 50 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　設定をデフォルトの 250 に戻します。

```
sensor(config-net-gen)# default max-interfaces
```

ステップ 7　デフォルト設定を確認します。

```
sensor(config-net-gen)# show settings

   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ブロックしないアドレスの設定

ブロックしないホストとネットワークを設定するには、サービス ネットワーク アクセス サブモードで **never-block-hosts** コマンドおよび **never-block-networks** コマンドを使用します。

次のオプションが適用されます。

- *ip_address*：ブロックしないデバイスの IP アドレス。
- *ip_address/netmask*：ブロックしないネットワークの IP アドレス。形式は、A.B.C.D./nn です。

手動であってもブロックされるべきではないホストおよびネットワークを識別できるように、センサーをチューニングする必要があります。これは、信頼されたネットワーク デバイスの通常の動作が、攻撃として扱われる可能性があるためです。このようなデバイスや信頼された内部ネットワークもブロックする必要はありません。

1 つのホストまたはネットワーク全体を指定できます。

ブロッキング デバイスでブロックしないアドレスを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ブロックしないアドレスを定義します。

- 1 つのホストの場合

  ```
  sensor(config-net-gen)# never-block-hosts 10.16.0.0
  ```

- ネットワーク全体の場合

  ```
  sensor(config-net-gen)# never-block-networks 10.0.0.0/8
  ```

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 2)
      -----------------------------------------------
         ip-address: 10.16.0.0
         -----------------------------------------------
         ip-address: 11.11.11.11
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 2)
      -----------------------------------------------
         ip-address: 10.0.0.0/8
         -----------------------------------------------
         ip-address: 12.12.0.0/16
--MORE--
```

ステップ 6　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 7　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ユーザ プロファイルの設定

センサーで管理する他のデバイスのユーザ プロファイルを設定するには、サービス ネットワーク アクセス サブモードで **user-profiles** *profile_name* コマンドを使用します。ユーザ プロファイルには、ユーザ ID、パスワード、およびイネーブル パスワードの情報が含まれます。たとえば、同じパスワードとユーザ名を使用するルータはすべて 1 つのユーザ プロファイルの下にまとめることができます。

（注） デバイスへのログインにユーザ名やパスワードが不要である場合は、値を設定しないでください。

（注） ブロッキング デバイスを設定する前に、ユーザ プロファイルを作成する必要があります。

ユーザ プロファイルを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ユーザ プロファイル名を作成します。

```
sensor(config-net)# user-profiles PROFILE1
```

ステップ 4　このユーザ プロファイルのユーザ名を入力します。

```
sensor(config-net-use)# username username
```

ステップ 5　ユーザのパスワードを指定します。

```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```

ステップ 6　ユーザのイネーブル パスワードを指定します。

```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

ステップ 7　設定を確認します。

```
sensor(config-net-use)# show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-use)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ブロッキング デバイスおよびレート制限デバイスの設定

この項では、センサーがブロックやレート制限に使用するデバイスの設定方法について説明します。取り上げる事項は次のとおりです。

センサーがデバイスを管理するしくみ

ARC は、Cisco ルータおよびスイッチ上の ACL を使用してこれらのデバイスを管理します。これらの ACL は、次のもので構成されています。

（注）　ACL はレート制限のあるデバイスには適用されません。

1. センサーの IP アドレスまたは NAT アドレス（指定されている場合）を記述した **permit** 行。

   （注）　センサーのブロックを許可する場合は、この行は ACL に表示されません。

2. Pre-Block ACL（指定されている場合）

   この ACL はすでにデバイスに存在している必要があります。

   （注）　ARC はこの ACL の行を読み取り、その行を ACL の先頭にコピーします。

3. すべてのアクティブなブロック
4. 次のいずれか
   - Post-Block ACL（指定されている場合）

     この ACL はすでにデバイスに存在している必要があります。

     （注）　ARC はこの ACL の行を読み取り、その行を ACL の最後にコピーします。

     （注）　一致しなかったすべてのパケットを許可する場合は、ACL の最後の行を必ず **permit ip any any** にしてください。

   - **permit ip any any**（Post-Block ACL が指定されている場合は使用されません）

ARC は、2 つの ACL を使用してデバイスを管理します。一時点でアクティブになるのは、どちらか 1 つだけです。ARC は、オフラインになっている ACL の名前を使用して新しい ACL を作成し、それをインターフェイスに適用します。その後、次のサイクルでは、ARC はこの逆のプロセスを実行します。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新規 ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。

Pre-Block または Post-Block ACL を変更する必要がある場合は、次の手順を実行します。

1. センサーでのブロッキングをディセーブルにします。
2. デバイスのコンフィギュレーションを変更します。
3. センサーでのブロッキングを再度イネーブルにします。

ブロッキングが再度有効になると、センサーは新しいデバイス コンフィギュレーションを読み取ります。手順については、P.10-8 の「ブロッキング プロパティの設定」を参照してください。

注意　1 つのセンサーで複数のデバイスを管理することはできますが、複数のセンサーで 1 つのデバイスを制御することはできません。このような場合は、マスター ブロッキング センサーを使用します。手順については、P.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」を参照してください。

センサーで Cisco ルータを管理するための設定

この項では、センサーを設定して Cisco ルータを管理する方法について説明します。取り上げる事項は次のとおりです。

ルータと ACL

Pre-Block ACL と Post-Block ACL は、ルータのコンフィギュレーション内に作成し、保存します。これらの ACL は名前付きまたは番号付きの拡張 IP ACL にする必要があります。ACL の作成の詳細については、ルータのマニュアルを参照してください。

（注）　Pre-Block および Post-Block ACL は、レート制限には適用されません。

Pre-Block ACL と Post-Block ACL の各フィールドに、ルータにすでに設定されている ACL の名前を入力します。

Pre-Block ACL は、主にブロック対象外のものを許可するために使用されます。この ACL を使用してパケットがチェックされるとき、最初に一致する行によってアクションが決まります。最初に一致する行が Pre-Block ACL の許可の行である場合、ACL の後の方に（自動ブロックの）拒否の行があっても、そのパケットは許可されます。Pre-Block ACL は、ブロックによって生じる拒否の行よりも優先されます。

Post-Block ACL は、同じインターフェイスまたは方向に対して、追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合、その ACL を Post-Block ACL として使用できます。Post-Block ACL がない場合、センサーは新しい ACL の最後に **permit ip any any** を挿入します。

センサーが起動すると、2 つの ACL の内容が読み込まれます。そして、次のエントリを持った 3 つ目の ACL が作成されます。

- センサーの IP アドレスの **permit** 行
- Pre-Block ACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Pre-Block ACL のすべての設定行のコピー

センサーは新しい ACL を、指定したインターフェイスと方向に適用します。

（注） 新しい ACL がルータのインターフェイスまたは方向に適用されると、そのインターフェイスまたは方向に対する他の ACL が適用されなくなります。

センサーで Cisco ルータを管理するための設定

センサーを設定して Cisco ルータを管理し、ブロッキングやレート制限を実行するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ARC によって制御されたルータの IP アドレスを設定します。

```
sensor(config-net)# router-devices ip_address
```

ステップ 4　P.10-24 の「ユーザ プロファイルの設定」で作成した論理デバイス名を入力します。

```
sensor(config-net-rou)# profile-name user_profile_name
```

何を入力しても ARC によって受け入れられます。ユーザ プロファイルが存在するかどうかはチェックされません。

ステップ 5　センサーにアクセスするために使用する方法を指定します。

```
sensor(config-net-rou)# communication [telnet | ssh-des | ssh-3des]
```

指定しない場合は、SSH 3DES が使用されます。

（注）　DES または 3DES を使用している場合は、コマンド **ssh host-key** *ip_address* を使用して鍵を受け入れる必要があります。そうしないと、ARC はデバイスに接続できません。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 6　センサーの NAT アドレスを指定します。

```
sensor(config-net-rou)# nat-address nat_address
```

（注）　これによって ACL の最初の行の IP アドレスがセンサーのアドレスから NAT アドレスへ変更されます。これは、管理対象のサービスで設定された NAT アドレスではありません。センサーは、中間デバイスによってこのアドレスに変換されます。つまり、これは、センサーと管理対象デバイスの間のアドレスです。

ステップ 7　ルータで、ブロッキングまたはレート制限（あるいはその両方）を実行するかどうかを指定します。

（注）　デフォルトはブロッキングです。ルータでブロッキングだけを実行する場合は、応答機能を設定する必要はありません。

a.　レート制限だけの場合は、次のコマンドを実行します。

```
sensor(config-net-rou)# response-capabilities rate-limit
```

b.　ブロッキングとレート制限の両方を実行する場合は、次のコマンドを実行します。

```
sensor(config-net-rou)# response-capabilities block|rate-limit
```

ステップ 8　インターフェイス名と方向を設定します。

```
sensor(config-net-rou)# block-interfaces interface_name [in | out]
```

注意　インターフェイスの名前は、インターフェイスの完全な名前か、**interface** コマンドで使用したときにルータで認識される省略名である必要があります。

ステップ 9　（オプション）Pre-ACL 名を追加します（ブロッキングのみ）。

```
sensor(config-net-rou-blo)# pre-acl-name pre_acl_name
```

ステップ 10　（オプション）Post-ACL 名を追加します（ブロッキングのみ）。

```
sensor(config-net-rou-blo)# post-acl-name post_acl_name
```

ステップ 11　設定を確認します。

```
sensor(config-net-rou-blo)# exit
sensor(config-net-rou)# show settings
   ip-address: 10.89.127.97
   -----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      -----------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         -----------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      response-capabilities: block|rate-limit default: block
   -----------------------------------------------
sensor(config-net-rou)#
```

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-rou)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定

この項では、センサーを設定して Cisco スイッチを管理する方法について説明します。取り上げる事項は次のとおりです。

スイッチと VACL

ARC のブロッキングを設定するときには、Cisco Catalyst ソフトウェアを実行している場合にはスイッチ自体にある VACL を、また、Cisco IOS ソフトウェアを実行している場合には MSFC 上またはスイッチ自体にあるルータの ACL を使用できます。この項では、VACL を使用したブロッキングについて説明します。VACL を使用するスイッチでレート制限を実行するように設定することはできません。

ルータの ACL を使用したブロッキングについては、P.10-27 の「センサーで Cisco ルータを管理するための設定」を参照してください。

Catalyst 6500 シリーズ スイッチ上でブロッキング インターフェイスを設定し、ブロックするトラフィックの VLAN を指定する必要があります。

Pre-Block VACL と Post-Block VACL は、スイッチのコンフィギュレーション内に作成し、保存します。これらの VACL は名前付きまたは番号付きの拡張 IP VACL にする必要があります。VACL の作成の詳細については、スイッチのマニュアルを参照してください。

Pre-Block VACL と Post-Block VACL の各フィールドに、スイッチですでに設定されている VACL の名前を入力します。

Pre-Block VACL は、主にブロック対象外のものを許可するために使用されます。VACL を使用してパケットがチェックされる場合は、最初に一致する行によってアクションが決まります。最初に一致する行が Pre-Block VACL の許可の行である場合、VACL の後の方に（自動ブロックの）拒否の行があっても、そのパケットは許可されます。Pre-Block VACL は、ブロックによって生じる拒否の行よりも優先されます。

Post-Block VACL は、同じ VLAN で追加的なブロッキングまたは許可を行う場合に最適です。センサーが管理する VLAN に既存の VACL がある場合、その VACL を Post-Block VACL として使用できます。Post-Block VACL がない場合、センサーは新しい VACL の最後に **permit ip any any** を挿入します。

（注） IDSM-2 は、新しい VACL の最後に **permit ip any any capture** を挿入します。

センサーが起動すると、2 つの VACL の内容が読み込まれます。そして、次のエントリを持った 3 つ目の VACL が作成されます。

- センサーの IP アドレスの **permit** 行
- Pre-Block VACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block VACL のすべての設定行のコピー

センサーは、新しい VACL を指定した VLAN に適用します。

（注） スイッチの VLAN に新しい VACL が適用されると、該当の VLAN に対して他のすべての VACL は適用されなくなります。

センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定

センサーを設定して Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ARC によって制御されたルータの IP アドレスを設定します。

```
sensor(config-net)# cat6k-devices ip_address
```

ステップ 4　P.10-24 の「ユーザ プロファイルの設定」で作成したユーザ プロファイル名を入力します。

```
sensor(config-net-cat)# profile-name user_profile_name
```

（注）　何を入力しても ARC によって受け入れられます。これは、論理デバイスが存在するかどうかをチェックしません。

ステップ 5　センサーにアクセスするために使用する方法を指定します。

```
sensor(config-net-cat)# communication [telnet | ssh-des/ | sh-3des]
```

指定しない場合は、SSH 3DES が使用されます。

（注）　DES または 3DES を使用している場合は、コマンド **ssh host-key** *ip_address* を使用して鍵を受け入れる必要があります。そうしないと、ARC はデバイスに接続できません。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 6　センサーの NAT アドレスを指定します。

```
sensor(config-net-cat)# nat-address nat_address
```

（注）　これによって ACL の最初の行の IP アドレスがセンサーのアドレスから NAT アドレスへ変更されます。これは、管理対象のサービスで設定された NAT アドレスではありません。センサーは、中間デバイスによってこのアドレスに変換されます。つまり、これは、センサーと管理対象デバイスの間のアドレスです。

ステップ 7　VLAN 番号を指定します。

```
sensor(config-net-cat)# block-vlans vlan_number
```

ステップ 8　（オプション）Pre-VACL 名を追加します。

```
sensor(config-net-cat-blo)# pre-vacl-name pre_vacl_name
```

ステップ 9　（オプション）Post-VACL 名を追加します。

```
sensor(config-net-cat-blo)# post-vacl-name post_vacl_name
```

ステップ 10　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-cat-blo)# exit
sensor(config-net-cat)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 11　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

センサーで Cisco ファイアウォールを管理するための設定

センサーを設定して Cisco ファイアウォールを管理するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ARC によって制御されたファイアウォールの IP アドレスを設定します。

```
sensor(config-net)# firewall-devices ip_address
```

ステップ 4　P.10-24 の「ユーザ プロファイルの設定」で作成したユーザ プロファイル名を入力します。

```
sensor(config-net-fir)# profile-name user_profile_name
```

（注）　何を入力しても ARC によって受け入れられます。これは、論理デバイスが存在するかどうかをチェックしません。

ステップ 5　センサーにアクセスするために使用する方法を指定します。

```
sensor(config-net-fir)# communication [telnet | ssh-des | sh-3des]
```

指定しない場合は、SSH 3DES が使用されます。

（注）　DES または 3DES を使用している場合は、コマンド **ssh host-key** *ip_address* を使用して鍵を受け入れる必要があります。そうしないと、ARC はデバイスに接続できません。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 6　センサーの NAT アドレスを指定します。

```
sensor(config-net-fir)# nat-address nat_address
```

（注）　これによって ACL の最初の行の IP アドレスがセンサーのアドレスから NAT アドレスへ変更されます。これは、管理対象のサービスで設定された NAT アドレスではありません。センサーは、中間デバイスによってこのアドレスに変換されます。つまり、これは、センサーと管理対象デバイスの間のアドレスです。

ステップ 7　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-fir)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 8　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

センサーをマスター ブロッキング センサーとして使用するための設定

ブロッキング要求は、複数のセンサー（ブロッキング転送センサー）から、1 つ以上のデバイスを制御するマスター ブロッキング センサーに転送できます。マスター ブロッキング センサーは、1 つ以上のセンサーに代わって 1 つ以上のデバイスのブロッキングを管理するセンサーで実行される ARC です。マスター ブロッキング センサーの ARC は、他のセンサーで実行されている ARC の要求により、デバイスのブロッキングを制御します。

注意　2 つのセンサーが同一のデバイスでブロッキングやレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーを、デバイス管理のためのマスター ブロッキング センサーとして設定します。それにより、もう一方のセンサーはマスター ブロッキング センサーに要求を転送できます。

（注）　マスター ブロッキング センサーを追加する場合は、センサーごとにブロックするデバイスの数を減らしてください。たとえば、10 のファイアウォールと 10 のルータでブロッキングを行い、ブロックするインターフェイス / 方向がそれぞれ 1 つずつある場合は、そのうちの 10 をセンサーに割り当て、残りの 10 をマスター ブロッキング センサーに割り当てます。

また、マスター ブロッキング センサーは、レート制限を転送することもできます。

これには、ブロッキング転送センサーで、どのリモート ホストがマスター ブロッキング センサーであるかを特定し、マスター ブロッキング センサーではブロッキング転送センサーをアクセス リストに追加する必要があります。

マスター ブロッキング センサーで Web 接続に TLS が必要である場合は、ブロッキング転送センサーの ARC がマスター ブロッキング センサーであるリモート ホストの X.509 証明書を受け入れるように設定する必要があります。センサーでは、デフォルトで TLS がイネーブルになっていますが、このオプションは変更可能です。

（注）　通常、マスター ブロッキング センサーは、ネットワーク デバイスを管理するために設定されます。ブロッキング転送センサーは、通常は他のネットワーク デバイスの管理目的では設定されませんが、設定することはできます。

ブロッキングやレート制限用に設定されたデバイスが存在しない場合であっても、ブロッキングやレート制限を実行するように設定されたセンサーは、ブロッキング要求やレート制限要求をマスター ブロッキング センサーに転送できます。イベント アクションとしてブロッキング要求やレート制限要求が設定されたシグニチャが発生すると、センサーはそのブロッキング要求またはレート制限要求をマスター ブロッキング センサーに転送し、そこでブロッキングやレート制限が実行されます。

注意　デバイス上のすべてのブロッキング インターフェイスは、1 つのセンサーのみで制御する必要があります。

マスター ブロッキング センサーを設定するには、サービス ネットワーク アクセス サブモードで `master-blocking-sensors` *mbs_ip_address* コマンドを使用します。

次のオプションが適用されます。

- *mbs_ip_address*：ブロック要求を転送するセンサーの IP アドレス。
- **password**：ブロック要求を転送するセンサーのアカウント パスワード。
- **port**：ブロック要求を転送するセンサーのポート。
- **tls [true | false]**：リモート センサーで TLS が必要な場合は true に設定し、そうでない場合は false に設定します。
- **username**：ブロック要求を転送するセンサーのアカウント名。

センサーの ARC がマスター ブロッキング センサーにブロックを転送するように設定するには、次の手順を実行します。

ステップ 1　マスター ブロッキング センサーとブロッキング転送センサーの両方で管理者特権を持つアカウントを使用して、CLI にログインします。

ステップ 2　両方のセンサーでコンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　必要に応じて TLS を設定します。

a. マスター ブロッキング センサーで、TLS が必要かどうかと、使用されるポート番号を確認します。

```
sensor(config)# service web-server
sensor(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)#
```

`enable-tls` が true の場合は、ステップ b に進みます。

b. ブロッキング転送センサーで、このセンサーがマスター ブロッキング センサーの X.509 証明書を受け入れるように設定します。

```
sensor(config-web)# exit
sensor(config)# tls trusted-host ip-address mbs_ip_address port port_number
```

例

```
sensor(config)# tls trusted-host ip-address 10.0.0.0 port 8080
Certificate MD5 fingerprint is
F4:4A:14:BA:84:F4:51:D0:A4:E2:15:38:7E:77:96:D8Certificate SHA1 fingerprint is
84:09:B6:85:C5:43:60:5B:37:1E:6D:31:6A:30:5F:7E:4D:4D:E8:B2
Would you like to add this to the trusted certificate table for this host?[yes]:
```

（注）　証明書のフィンガープリントに基づいて証明書を受け入れるように求めるプロンプトが表示されます。センサーは自己署名証明書のみを提示します（公認の認証局の証明書ではありません）。マスター ブロッキング センサーのホストでセンサーにログインし、**show tls fingerprint** コマンドを入力して、このホストの証明書のフィンガープリントと一致することを確認することによって、ホスト センサーの証明書を検証することができます。

ステップ 4　`yes` を入力して、マスター ブロッキング センサーの証明書を受け入れます。

ステップ 5　ネットワーク アクセス モードに入ります。

```
sensor(config)# service network-access
```

ステップ 6　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 7　マスター ブロッキング センサーのエントリを追加します。

```
sensor(config-net-gen)# master-blocking-sensors mbs_ip_address
```

ステップ 8　マスター ブロッキング センサー ホストの管理アカウントのユーザ名を指定します。

```
sensor(config-net-gen-mas)# username username
```

ステップ 9　ユーザのパスワードを指定します。

```
sensor(config-net-gen-mas)# password
Enter password []: *****
Re-enter mbs-password []: *****
sensor(config-net-gen-mas)#
```

ステップ 10　ホストの HTTP 通信用のポート番号を指定します。

```
sensor(config-net-gen-mas)# port port_number
```

指定しない場合、デフォルトは 80/443 になります。

ステップ 11　ホストが TLS/SSL を使用するかどうかのステータスを設定します。

```
sensor(config-net-gen-mas)# tls [true | false]
sensor(config-net-gen-mas)
```

（注）　この値を true に設定する場合は、コマンド **tls trusted-host ip-address** *mbs_ip_address* を使用する必要があります。

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen-mas)# exit
sensor(config-net-gen)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ステップ 14 マスター ブロッキング センサーで、アクセス リストにブロック転送センサーの IP アドレスを追加します。手順については、P.4-6 の「アクセス リストの変更」を参照してください。

手動ブロッキングの設定

ホストまたはネットワークを手動でブロックするには、サービス ネットワーク アクセス サブモードで **block-hosts** コマンドおよび **block-networks** コマンドを使用します。手動ブロックを設定する前に、ブロッキングを設定しておく必要があります。また、ブロックされているホストとネットワークのリストを表示することもできます。

（注） CLI での手動ブロックでは実際にコンフィギュレーションが変更されるため、ブロックは永続的です。期間を限定した手動ブロックを実行することはできません。CLI で作成したブロックを IPS マネージャを使用して削除することはできません。手動ブロックは CLI で削除する必要があります。

注意 手動ブロッキングは、使用するとしても最小限にすることをお勧めします。

ホストまたはネットワークを手動でブロックするには、次の手順を実行します。

ステップ 1 管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2 ネットワーク アクセス モードに入ります。

```
sensor# configuration terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3 汎用モードに入ります。

```
sensor (config-net)# general
sensor(config-net-gen)#
```

ステップ 4 手動ブロックを開始します。

a. ホストの IP アドレスの場合

```
sensor(config-net-gen)# block-hosts ip_address
```

b. ネットワークの IP アドレスの場合

```
sensor(config-net-gen)# block-networks ip_address/netmask
```

ip_address/netmask の形式は、A.B.C.D/nn です。

例

```
sensor (config-net-gen)# block-networks 10.0.0.0/8
```

（注）　手動ブロックは、CLI で終了しない限り永続します。

ステップ 5　手動ブロックを終了するには、次の操作を実行します。

```
sensor (config-net-gen)# no block-hosts ip_address
```

ステップ 6　ネットワーク アクセス サブモードを終了します。

```
sensor (config-net-gen)# exit
sensor (config-net)# exit
sensor(config)# exit
sensor#
```

ブロックされたホストと接続のリストの入手

ブロックされたホストとブロックされた接続のリストを入手するには、**show statistics** コマンドを使用します。

ブロックされたホストと接続のリストを入手するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC の統計情報を確認します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.1.1.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.1.1.1
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   BlockedAddr
      Host
         IP = 192.168.1.1
         Vlan =
         ActualIp =
         BlockMinutes = 80
         MinutesRemaining = 76
```

Host エントリに、ブロックされているホストと、ブロックされている時間が示されます。